



Docket No.: 62807-173

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of : Customer Number: 20277
Koichi TANIMOTO, et al. : Confirmation Number: 9181
Serial No.: 10/801,115 : Group Art Unit: 2131
Filed: March 16, 2004 : Examiner:
For: VERIFICATION RESULT RECORDING METHOD AND APPARATUS FOR
CREATING SIGNATURE VERIFICATION LOG

TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Mail Stop CPD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

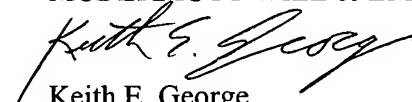
At the time the above application was filed, priority was claimed based on the following application:

Japanese Patent Application No. JP 2004-028794, filed on February 5, 2004.

A copy of each priority application listed above is enclosed.

Respectfully submitted,

MCDERMOTT WILL & EMERY LLP


Keith E. George
Registration No. 34,111

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 KEG:gav
Facsimile: (202) 756-8087
Date: July 28, 2004

10/801,115

July 28, 2004

日本国特許庁
JAPAN PATENT OFFICE

McDermott Will & Emery LLP

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日
Date of Application: 2004年 2月 5日

出願番号
Application Number: 特願2004-028794

ST. 10/C]: [JP2004-028794]

出願人
Applicant(s): 株式会社日立製作所

2004年 3月31日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

BEST AVAILABLE COPY

【書類名】 特許願
【整理番号】 K03017551A
【あて先】 特許庁長官殿
【国際特許分類】 G09C 1/00
【発明者】
 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所
 システム開発研究所内
 【氏名】 谷本 幸一
【発明者】
 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所
 システム開発研究所内
 【氏名】 宮崎 邦彦
【発明者】
 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所
 システム開発研究所内
 【氏名】 伊藤 信治
【発明者】
 【住所又は居所】 東京都江東区新砂一丁目 6 番 2 7 号 株式会社日立製作所公共シ
 ステム事業部内
 【氏名】 大本 周広
【特許出願人】
 【識別番号】 000005108
 【氏名又は名称】 株式会社 日立製作所
【代理人】
 【識別番号】 100075096
 【弁理士】
 【氏名又は名称】 作田 康夫
【選任した代理人】
 【識別番号】 100100310
 【弁理士】
 【氏名又は名称】 井上 学
【国等の委託研究の成果に係る記載事項】 国等の委託研究の成果に係る特許出願（平成
 1 5 年度通信・放送機構「次世代証拠基板技術に関する研究開発
 」委託研究、産業活力再生特別措置法第 3 0 条の適用を受けるも
 の）
【手数料の表示】
 【予納台帳番号】 013088
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1

【書類名】 特許請求の範囲**【請求項 1】**

署名者側装置と、検証者側装置と、公開機関側装置とからなる署名システムにおいて、署名の検証に関わる情報を記録した検証ログを作成する検証結果記録方法であって、
前記署名者側装置は、
作成した署名に関する署名記録を、連鎖関係を伴って署名者側署名履歴として記録し、
前記公開機関側装置は、
前記署名者側装置から預託された前記署名記録を公開し、
預託された複数の署名記録を、連鎖関係を伴って公開機関側署名履歴として記録し、
前記公開機関側署名履歴中の所定の署名記録を新聞公開署名記録として公開し、
前記検証者側装置は、
前記公開機関側署名履歴を用いて、
前記新聞公開署名記録から前記署名者側装置が公開を預託した前記署名記録まで、署名間の連鎖関係の整合性が取れていることを検証し、
前記署名者側署名履歴を用いて、
前記署名者側装置が公開を預託した署名記録から前記検証対象署名に関わる署名記録まで、署名間の連鎖関係の整合性が取れていることを検証し、
前記検証に利用したデータを検証ログとして記録する、
ことを特徴とする検証結果記録方法。

【請求項 2】

請求項 1 記載の検証結果記録方法であって、
前記検証ログに記録される前記検証に利用したデータは、
前記検証対象署名と、
前記署名者側署名履歴と、
前記公開機関側署名履歴と、
前記新聞公開署名記録である、
ことを特徴とする検証結果記録方法。

【請求項 3】

請求項 2 記載の検証結果記録方法であって、
前記検証ログから、前記検証に利用したデータである、前記検証対象署名と、前記署名者側署名履歴と、前記公開機関側署名履歴と、前記新聞公開署名記録とを抽出し、
抽出した前記検証に利用したデータを利用して、前記新聞公開署名記録から前記検証対象署名に関わる署名記録まで、署名間の連鎖関係の整合性が取れていることを検証することにより、検証ログを検証すること
を特徴とする検証結果記録方法。

【請求項 4】

署名検証を行う検証者側装置であって、
署名者の公開鍵を用いて検証対象署名の検証を行う受信処理と、
新聞公開署名記録を起点として、前記検証対象署名までの連鎖関係を、署名者側署名履歴と公開機関側署名履歴とを用いて検証する検証処理と、
前記検証処理に利用したデータから検証ログを作成し記録する検証記録保存処理と、を
実行する
ことを特徴とする検証者側装置。

【請求項 5】

署名の信頼性向上処理を行う公開機関側装置であって、
署名者側装置から預託された署名記録を公開する公開処理と、
前記署名者側装置に署名記録の公開を催促する公開催促処理と、
前記署名者側装置に対して、他の署名者側装置から預託された署名記録を公開したことを通知する公開通知処理と、
前記署名者側装置に代わって、検証対象署名を、検証に必要なデータを収集して検証し

、検証ログを作成して検証結果を通知する検証代行処理と、を実行することを特徴とする公開機関側装置。

【請求項 6】

請求項 5 記載の公開機関側装置であって、
前記公開処理として、
署名者側装置からより公開を預託された署名記録を公開する公開処理と、
公開した前記署名記録に関わる情報を記録する公開情報登録処理と、
公開した前記署名記録に関して、他の署名者側装置から公開通知依頼を受け取っていたかどうかを確認する通知依頼有無確認処理と、
公開した前記署名記録に関して前記公開通知依頼を受け取っていれば、前記他の署名者側装置へ通知する公開通知処理と、を実行することを特徴とする公開機関側装置。

【請求項 7】

請求項 5 記載の公開機関側装置であって、
前記公開催促処理は、
署名記録の公開を催促すべき署名者を特定する対象者抽出処理と、
署名記録の公開を催促する催促文書を前記特定した署名者が利用する署名者側装置に送信する催促書送信処理と、
前記催促文書を送信したことを記録する催促情報登録処理と、
を実行することを特徴とする公開機関側装置。

【請求項 8】

請求項 5 記載の公開機関側装置であって、
前記公開通知処理は、
前記他の署名者側装置から前記公開通知依頼を受け取り、前記公開通知依頼の内容をデータベースに記録する通知依頼内容登録処理と、
前記通知依頼内容を記録した前記データベースから、通知依頼元である前記他の署名者側装置の情報を抽出する通知依頼者抽出処理と、
前記通知依頼元である前記他の署名者側装置に、通知依頼対象署名者による公開署名記録が公開されたことを通知する通知書送信処理と、
を実行することを特徴とする公開機関側装置。

【請求項 9】

請求項 5 記載の公開機関側装置であって、
前記検証代行処理は、
署名者側装置から検証代行の依頼を受け付ける検証代行依頼受取処理と、
検証依頼された検証対象署名について、検証に必要な公開署名記録、署名履歴を収集する検証データ収集処理と、
前記検証データ収集処理によって収集したデータを用いて、検証依頼された前記検証対象署名を検証する署名検証処理と、
前記検証結果、および前記検証に利用したデータを記録した検証ログを作成し、検証依頼元である前記署名者側装置に送付する検証ログ発行処理と、
依頼された前記検証対象署名について、検証状況を前記データベースに記録する検証状況登録処理と、
依頼された前記検証代行処理について、前記検証状況を確認する検証状況確認処理と、
を実行することを特徴とする公開機関側装置。

【書類名】 明細書**【発明の名称】** 署名検証ログを作成する検証結果記録方法とその装置**【技術分野】****【0001】**

本発明は、デジタル署名技術に関する。

【背景技術】**【0002】**

デジタル署名（以下、署名という）の証拠性を高める技術として、署名作成の際に、その時点までの署名履歴情報を反映させ、作成した署名に関わる情報を、署名記録として新たに署名履歴に追加する手法がある（例えば、特許文献1または特許文献2参照）。この方法により作成した署名は連鎖構造を持ち、改竄は困難となる。検証の際は、署名に対する検証の他に、連鎖の検証も行うことにより、改竄に対して厳密な検証が行える。この技術は、長期に渡って電子文書の証拠性を維持することを可能にするもので、ヒステリシス署名技術と呼ばれる。

【0003】

この技術においては、署名の検証を行う場合には、信頼できる署名から連鎖が繋がっている署名は全て信頼できると判断する。連鎖の検証も含めた厳密な署名検証に必要なデータは、検証対象署名、検証対象データ、および署名履歴である。この技術では、過去の署名を記録したこの署名履歴が、証拠性維持のよりどころとなっている。また、連鎖検証の起点となる信頼できる署名を作成するために、署名履歴の一部を第三者機関である公開機関を通じて公開するという方法が考えられている。

【0004】

【特許文献1】 特開2001-331104号公報

【0005】

【特許文献2】 特開2001-331105号公報

【発明の開示】**【発明が解決しようとする課題】****【0006】**

上記技術において、何らかの理由で署名履歴が失われてしまうと、以前には検証できていた署名の検証も困難となってしまう。従って、過去に少なくとも一度検証できていた署名については、署名履歴が失われたとしてもその証拠性が保証されることが望ましい。

【課題を解決するための手段】**【0007】**

本発明は、過去に検証した署名について、その証拠性を長期に渡って保証する技術を提供する。具体的には、検証の際に検証に利用したデータをログとして残し、それを長期にわたる保証において利用する。

【0008】

すなわち、本発明は、ヒステリシス署名技術を利用して作成した署名を検証した場合に、検証した署名の証拠性を長期に渡って維持できる検証記録保存機能を提供する。

【0009】

本発明において、「署名記録」とは、作成あるいは受信した個々の署名から作られる署名情報であり、「署名履歴」とは、複数の「署名記録」が保存されたファイルを指す。また、署名履歴中の署名記録は、所定の間隔を置いて、その時点での最新のものが公開機関を通して、公開され、公開された署名記録は、公開機関によりその信頼性が保証されているものとする。

【0010】

本発明では、長期経過後のヒステリシス署名技術に基づく署名を検証する際には、署名履歴中の公開機関側装置によって信頼性が保証された署名記録から、検証対象署名の署名記録まで連鎖の整合性が取れているかどうかを検証する。本発明の検証記録保存機能は、検証の際に利用した署名記録、公開機関側装置に公開した署名記録、および検証対象署名

を検証ログに記録する。

【0011】

これにより、たとえ署名履歴が消われた場合であっても、検証ログを調べることによって、それに記載されている署名の正当性を示すことができる。検証ログを、消失した場合であっても、再度、署名履歴の検証を行うことによって、検証ログを復元できる。

【0012】

また、本発明では、署名の信頼性を保証するための公開機関のサービス形態を提供する。すなわち、本発明では、公開機関側装置において、信頼できる署名を確実に作成して、連鎖検証に利用できるように、ユーザの公開忘れを防止するサービスや、ユーザに代わって検証を代行するなど、ユーザの利便性も考慮し、かつ信頼のある検証を行うサービスのための仕組みを提供する。このようなサービスの提供によって、一度検証した署名は、改めて検証することなくその証拠性を長期に渡って示すことができるようになる。

【発明の効果】

【0013】

本発明によれば、署名履歴などの証拠情報が消失してしまった場合でも、過去の検証時に作成された検証ログを利用して、証拠性を長期に渡って維持することができる。

【発明を実施するための最良の形態】

【0014】

図1は、本発明を適用した一実施形態におけるヒステリシス署名システムの概略図である。

【0015】

図示するように、本ヒステリシス署名システムは、署名作成、署名検証、検証記録保存、署名記録の公開を行うユーザ側装置101～103と、各ユーザから送られてきた署名記録を公開する公開機関側装置104とを含んで構成される。ユーザ側装置101～103と公開機関側装置104は、インターネットなどのネットワーク105を介して繋がっている。

【0016】

ユーザ側装置101～103は、図2に示すように、記憶装置202と、ネットワークを介して他の装置と通信を行うための通信装置204と、キーボードやマウスなどの入力装置205と、ディスプレイなどの表示装置206と、CPU201と、これらを接続するインタフェース203とから構成される。

【0017】

記憶装置202には、署名を作成して署名付き文書を送信する送信プログラム207と、署名付き文書を受信して署名を検証する受信プログラム208と、署名履歴の連鎖検証も含んだ検証を行う文書検証プログラム209と、検証した際に検証に使用したデータを検証ログに記録する検証記録保存プログラム210と、公開依頼書を作成して公開署名記録を公開機関側装置104に送信する公開依頼書送信プログラム211と、自分の署名履歴を他のユーザに送信する履歴送信プログラム212と、他のユーザから他のユーザの署名履歴を受信する履歴受信プログラム213と、署名履歴ファイル（署名履歴という）214と、ユーザ情報ファイル215と、他ユーザから受信した署名履歴を保存する他ユーザ署名履歴保存ファイル216が格納されている。

【0018】

以下の説明における各プログラム207～213の処理は、インタフェース203を介して呼び出された各プログラムをCPU201が実行することにより、ユーザ側装置101～103上で実現されるものである。各プログラムは、予め記憶装置202に格納されていてもよいし、ユーザ側装置101～103が利用可能な媒体を介して導入されてもよい。媒体とは、たとえば、公開機関側装置104に着脱可能な記憶媒体や、通信装置204に接続するネットワークまたはネットワークを伝搬する搬送波といった通信媒体を含む。

【0019】

また、これらのプログラムは、署名作成時に署名履歴情報を反映させるヒステリシス署名技術を利用している。ユーザ側装置は、署名者のユーザ側装置（以下、署名者側装置という）と検証者のユーザ側装置（以下、検証者側装置という）とに区別される。署名者側装置は署名を作成したユーザ側装置を表し、検証者側装置は、署名を検証するユーザ側装置を表す。ただし、署名者側装置が自分の作成した署名を検証する場合は、署名者側装置と検証者側装置は同一である。

【0020】

なお、公開機関側装置104の構成は、後に図8を用いて説明する。

【0021】

図3は、署名者のユーザ側装置101～103が送信文書307に対し署名308を作成した後、署名付き受信文書309を受信し署名検証した場合の署名履歴の様子を示したものである。この場合、ユーザ側装置101～103は、署名作成時は署名者側装置であり、署名付き文書受信時には、検証者側装置となる。署名作成時には、署名者側装置は、送信プログラム207の処理により、送信文書307と前回の署名記録313のハッシュ値に対して秘密鍵を作用させて署名308を作成する。作成後、前回の署名記録313と作成した署名308から、署名記録314を作成し、署名履歴311に追加する。

【0022】

署名受信時には、検証者側装置は、受信プログラム208の処理により、受信文書309に対する署名310を公開鍵を用いて検証する。検証後、前回の署名記録314のハッシュ値と署名310から署名記録315を作成し、署名履歴311に追加する。以上のように、署名作成時や署名受信時において、署名情報を記録した署名記録が作られる。前回の署名情報が次の署名作成に利用されるため、署名間に連鎖関係が生じる。通常の公開鍵を用いた署名検証に加えて、この連鎖関係を検証する（以降、連鎖検証と呼ぶ）ことにより、より確実な署名の検証を行うことができる。

【0023】

ユーザ側装置101～103における署名記録は、署名アルゴリズム等の情報を示す「識別番号301」、何番目に作られた署名記録であることを示す「署名番号302」、署名作成（送信）時に作成した署名記録か、署名検証（受信）時に作成した署名記録かを表す「種別303」、連鎖検証に利用する「前回署名記録のハッシュ値304」、署名作成時のみ記録する「署名作成対象文書のハッシュ値（文書のハッシュ値という）305」、「署名or受信署名記録情報306」（署名作成時は、作成した署名。署名検証時は、受信した署名の署名番号とその署名に対する署名記録のハッシュ値を結合したもの）を含んで構成される。なお、どの署名がどの署名記録中に残っているか判別するために、署名作成時においては、署名履歴に今回新たに追加される署名記録の署名番号を、作成した署名に付加する。作成された署名記録が順に記録されたファイルが署名履歴である。

【0024】

ユーザ側装置101～103は、予め定めた規則、たとえば定期的に最新の署名記録を公開機関側装置104などの信頼できる第三者機関側装置に預託する。具体的には、公開依頼書送信プログラム211の実行により、ユーザ側装置101～103は自身の署名履歴214から最新の署名記録を取得し、その署名記録を含んだ公開依頼書を公開機関側装置104に送信する。公開機関側装置104側では、受け取ったユーザ側装置101～103の署名記録を公開する。公開機関側装置104に預託され公開された署名記録を預託公開署名記録と呼ぶ。

【0025】

また、公開機関側装置104もヒステリシス署名を利用することで、ユーザの預託公開署名記録の正当性をより一層高めることができる。公開機関側装置104の公開の仕組みを図4に示す。

【0026】

公開機関側装置104は、ユーザ側装置101～103より預託公開署名記録が付加された公開依頼書408を受け取ると、公開プログラム809の処理により、その公開依頼

書 408 と前回の署名記録 412 のハッシュ値に対して公開機関側装置 104 の秘密鍵を作用させて署名 409 を作成する。

【0027】

また、その公開依頼書 408 に対して、公開依頼書ごとに決められる固有の公開IDを作成する。そして、作成した署名 409 と公開ID、および預託公開署名記録とから、署名記録 413 を作成し、公開機関側装置 104 の署名履歴 410 に記録する。最後に、預託公開署名記録と公開ID、および公開依頼書送信元のユーザ名（もしくはメールアドレス）とを公開する。

【0028】

公開先としては、掲載場所が限られる新聞よりは、Webなどが望ましい。公開IDは、公開依頼書ごとに固有であるので、公開IDによって、Webに公開された預託公開署名記録と公開機関側装置 104 の署名記録とを対応付けることができる。

【0029】

公開機関側装置 104 における署名記録は、署名アルゴリズム等の情報を示す「識別番号 401」、何番目に作られた署名記録であることを示す「署名番号 402」、連鎖検証に利用する「前回署名記録のハッシュ値 403」、「署名値 404」、公開依頼書ごとに作成された「公開ID 405」、公開した預託公開署名記録の署名番号「公開署名記録番号 406」、公開した預託公開署名記録のハッシュ値「預託公開署名記録のハッシュ値 407」を含んで構成される。この署名記録が順に記録されたファイルが公開機関側装置 104 の署名履歴 410 である。

【0030】

上記のような公開処理を行うことによって、公開機関側装置 104 は、公開した情報を履歴の中に記録しており、またその記録の間には連鎖関係が構築されている。そのため、定期的に公開機関側装置 104 の署名履歴 410 中の最新の署名記録（たとえば、最新の署名記録のハッシュ値）を新聞等、刊行物（以下、新聞と総称する）に公開して、信頼できるものとし、署名履歴の連鎖検証により公開機関自身が不正を行っていないことを証明することができる。なお、以下では、新聞等刊行物に公開した署名記録を新聞公開署名記録と呼ぶ。

【0031】

新聞公開署名記録は、後から取り消したり、改ざんしたりすることが非常に困難であるので、信頼性の高い署名記録であるといえる。検証者側装置が連鎖検証する際には、この新聞公開署名記録から、検証対象署名の署名記録までの連鎖を検証する。連鎖が確認できれば、検証対象署名の署名記録は、新聞公開署名記録と同等の信頼性があるといえ、正当性が保証される。

【0032】

ユーザ側装置における連鎖検証の手順を、図5に示す。

【0033】

検証者側装置は、署名者の公開鍵によって検証対象署名を検証した後、S527で、署名付き文書中の検証対象署名 501（図3の310に相当）（＝「署名3」）と、それに対応する署名番号（＝「3」）を持つ署名者側装置の署名履歴 502 中の、署名記録 503 の署名値 506（図3の306に相当）（＝「署名3」）とが一致するかどうか検証する。ここで、署名者側装置の署名履歴 502 は、検証前に署名者側装置より入手する。

【0034】

S528で、検証者側装置は、新聞公開署名記録 526 から、公開機関に預託されている署名者側装置の預託公開署名記録 513 に対応する署名者側装置の署名履歴 502 中の署名記録 509 までの検証を行う。具体的には、まず、署名者側装置の預託公開署名記録 513 について、それとともに公開されている公開ID（＝「358」）を取得し、次に公開機関側装置 104 の署名履歴において、その公開ID（＝「358」）が記録されている署名記録 518 の項目 519（図4の402に相当）署名番号（＝「87」）を取得する。

【0035】

次に、取得した署名番号「87」以降の署名番号を持つ新聞公開署名記録526（＝「署名番号96」）を新聞から取得する。そして、公開機関側装置104の署名履歴において、新聞公開署名記録526と同じ署名番号（＝「96」）を持つ署名記録524のハッシュ値と新聞公開署名記録526が一致するかどうか検証する。

【0036】

次に、公開機関側装置104の署名履歴において、署名記録524中の項目525（図4の403に相当）前回署名記録のハッシュ値（＝「H(P95)」）と、その1つ前の署名記録523のハッシュ値とが一致するかどうか検証する。ハッシュ関数を用いて署名記録と1つ前の署名記録との整合性を調べるこの処理を、公開機関側装置104の署名履歴について、新聞公開署名記録に対応する署名番号（＝「96」）を持つ署名記録524から、預託公開署名記録に対応する署名番号（＝「87」）を持つ署名記録518まで繰り返す。そして、公開機関側装置104の署名記録518中の項目522（図4の407に相当）公開署名記録のハッシュ値（＝「H(S20)」）と、預託公開署名記録513のハッシュ値とが一致するかどうか検証する。最後に、預託公開署名記録513と、それに対応する署名者側装置の署名履歴502中の署名記録509（＝署名番号「20」）とが一致するかどうか検証する。

【0037】

検証者側装置は、S528での検証に必要な署名者側装置の預託公開署名記録513、公開機関の署名履歴517、新聞公開署名記録526を、検証前に公開機関側装置は、および新聞より入手する。

【0038】

S529で、検証者側装置は、署名者側装置の署名履歴の署名記録509中の項目511（図3の304に相当）前回署名記録のハッシュ値（＝「H(S19)」）と、その1つ前の署名記録508のハッシュ値とが一致するかどうか検証する。ハッシュ関数を用いて署名記録と1つ前の署名記録との整合性を調べるこの処理を、預託公開署名記録513に対応する署名番号（＝「20」）を持つ署名記録509から、検証対象署名501に対応する署名番号（＝「3」）を持つ署名記録503まで繰り返す。

【0039】

文書検証プログラム209の処理によるS527、S528、S529の全ての検証が成功であれば、検証対象署名における連鎖検証は成功である。

【0040】

上記、連鎖検証に必要なデータは、「検証対象署名501（図3の304に相当）」、「署名履歴502（署名記録503、507～509）」、「預託公開署名記録513」、「公開機関側装置104の署名履歴517（署名記録518、523、524）」、「新聞公開署名記録526」である。そこで、検証者側装置は、検証記録保存プログラム210の処理により、S530において、この5つのデータを検証ログに記録する。作成した検証ログは、検証ログ保管領域217に保管する。

【0041】

検証ログの構成例を図6に示す。検証ログ601中、603（図3の310、図5の501に相当）は、検証対象署名であり、604～607は、連鎖検証に利用した検証対象署名の署名者側装置の署名記録である。また、608（図5の513に相当）は、預託公開署名記録であり、公開IDとともに記録される。610～612は公開機関側装置104の署名記録である。613（図5の526に相当）は新聞公開署名記録であり、署名番号とともに記録される。この他に、検証ログ作成日602や預託公開署名記録の公開場所609、新聞公開署名記録が記載されている新聞社名614、検証に利用した公開鍵615などの付加情報を記録しても良い。

【0042】

検証ログ601には、検証対象署名603（図3の310、図5の501に相当）について、連鎖検証を含む署名検証に必要なデータが記録されている。したがって、検証者側

装置は、このログ中に記載されたデータを用いて、図5を用いて説明した連鎖検証の手順を再度行うことによって、検証ログに記載された署名603（図3の310、図5の501に相当）の検証と検証ログの正当性の検証を行うことができる。すなわち、検証ログは、署名の正当性証明書であるともいえる。

【0043】

検証ログに記載された検証対象署名603（図3の310、図5の501に相当）が、署名記録604～607、預託公開署名記録608（図5の513に相当）、公開機関側装置104の署名記録610～612、新聞公開署名記録613、公開鍵615を用いて検証でき、かつ検証ログに記載された新聞公開署名記録613（図5の526に相当）が新聞に記載されているものと一致すれば、検証ログに記載されている検証対象署名603は正当であるといえる。本実施形態の方法によれば、例えば署名者側装置の署名履歴が消失してしまっても、検証者側装置は、検証ログから検証に利用したデータを抽出し、公開鍵を用いた署名検証および、S527、S528、S529の検証を行うことによって、検証ログに記載されている署名の正当性を提示することができる。

【0044】

また、検証ログの方を先に消失してしまった場合でも、検証者側装置は、再度連鎖検証を行い、検証記録保存機能を用いることによって、検証ログを再作成することができる。

【0045】

検証ログ601は、公開されても良いように、署名履歴には、秘密鍵漏洩やプライバシー漏洩に繋がる危険性があるような情報は含んでいないので、検証ログが公開されても、秘密鍵漏洩やプライバシー漏洩することはない。そのため、検証者側装置が、検証ログを公開して、第三者の手によって検証させることも可能である。

【0046】

また、検証ログが改ざんされた場合、検証対象署名603（図3の310、図5の501に相当）について、検証者側装置は、改ざんされてしまった後の検証ログを用いた検証は行えなくなるが、預託公開署名記録から検証対象署名へと繋がる連鎖の整合性は取れなくなるので、不正な署名の検証が成功となることはない。また、検証ログは、そこに記載されている検証対象署名のみに関する検証結果であるので、検証ログが改ざんされても、そこに記載されている署名以外の他の署名の検証結果に影響を及ぼしたりすることはない。

【0047】

検証ログは、ユーザ側装置（署名者側装置あるいは検証者側装置、またはその双方）が保管しても良いが、重要文書については、検証ログを、公的な信頼できる第三者機関に預ける、もしくは公的な信頼できる第三者機関側装置に署名してもらうことで、より安全性を高めることができる。検証ログには、秘密鍵漏洩やプライバシー漏洩に繋がる危険性があるような情報は含まれていないので、検証ログを預託することによって秘密鍵漏洩やプライバシー漏洩が生じる危険性はない。

【0048】

公開機関側装置104は、ユーザから署名記録を受け取り、それを公開する第三者機関側装置である。公開した署名記録を預託公開署名記録と呼ぶ。各ユーザにおいて、預託公開署名記録を、署名の連鎖検証の際の起点として利用することによって、預託公開署名記録から連鎖を辿ることができた署名は、公開機関側装置104に公開したのと同等の信頼性を得ることができ、署名の長期証拠性を保証することができる。

【0049】

また、公開機関側装置104は、図7に示す以下のようなサービスを提供してもよい。これによって、以下のような効果が得られる。

【0050】

上記実施例では、預託公開署名記録の公開のタイミングは、ユーザ側装置からの預託公開署名記録の送付に依存しているが、図7に示すサービスによれば、ユーザ側において公開するのを忘れても、連鎖検証が困難になることはない。

【0051】

また、署名の連鎖検証が可能となるのは、その署名が作成されて以降、署名者側装置が公開機関側装置104を利用して預託公開署名記録を作成した時点である。図7に示すサービスによれば、検証対象の署名の署名者側装置と検証者側装置が異なる場合であっても、検証者側装置は連鎖検証可能となったかどうかを知るためには、署名者側装置の署名記録が公開されたかどうかを確認する必要がなくなる。

【0052】

また、ヒステリシス署名の場合、署名の検証には、署名者側装置の署名履歴、署名者側装置の預託公開署名記録が必要であるが、図7に示すサービスによれば、検証対象の署名の署名者側装置と検証者側装置が異なる場合であっても、検証者がこれらを集める必要がなく、また、署名者が非協力的であっても、検証が可能である。

【0053】

また、図7に示すサービスに用いる公開機関側装置104の構成を図8に示す。

【0054】

公開機関側装置104は、図8に示すように、署名を作成して署名付き文書を送信する送信プログラム807と、署名付き文書を受信して署名を検証する受信プログラム808と、ユーザから受け取った預託公開署名記録705（図5の513に相当）をWeb等に公開する公開プログラム809と、一定期間公開が無いユーザに対して、公開催促書706を送信する公開催促プログラム810と、公開通知依頼書707を送ってきたユーザに対して、公開通知書708を送信する公開通知プログラム811と、検証対象署名付き検証依頼書709を送ってきたユーザに対して、検証対象署名を検証し、検証結果が書かれた検証ログを送付する検証代行プログラム812と、ユーザから署名履歴を受け取る履歴受信プログラム813と、各ユーザについての公開情報が記録された公開データベース814と、公開通知依頼書を送ってきたユーザについての情報と公開通知処理状況が記録された公開通知依頼データベース815と、検証代行について、検証代行依頼書を送ってきたユーザについての情報と検証代行処理状況が記録された検証状況データベース816と、ユーザから受け取った署名履歴を保管する署名履歴保管領域817と、ユーザから受け取った預託公開署名記録を保管する公開署名記録保管領域818と、ユーザから受け取った検証代行依頼書を保管する検証代行依頼書保管領域819と、公開機関側装置104が作成したあるいはユーザより預託された検証ログを保管する検証ログ保管領域820が格納されている記憶装置802と、ネットワークを介して他の装置と通信を行うための通信装置804と、キーボードやマウスなどの入力装置805と、ディスプレイなどの表示装置806と、CPU801と、これらを接続するインタフェース803とから構成される。

【0055】

以下の説明における各プログラムの処理は、CPU801が各プログラムを実行することにより、公開機関側装置104上で実現されるものである。各プログラムは、予め記憶装置802に格納されていてもよいし、公開機関側装置104が利用可能な媒体を介して導入されてもよい。媒体とは、たとえば、公開機関側装置104に着脱可能な記憶媒体や、通信装置804に接続するネットワークまたはネットワークを伝搬する搬送波といった通信媒体を含む。

【0056】

公開サービス701は、公開機関側装置104がユーザから預託公開署名記録705（図5の513に相当）を受け取り、それを自身のデータベースに保管、あるいはWebなどに公開するサービスである。ユーザは、本サービスを利用して、自身の署名履歴中に連鎖検証の際の起点となる信頼性の高い署名記録を生成することができる。

【0057】

公開処理の流れを図9に示す。

【0058】

公開機関側装置104は、公開サービス701を行う際、公開プログラム809により、以下のS901～S906の公開処理を行う。

【0059】

S901で公開機関側装置104はユーザより公開を依頼するデータ（預託公開署名記録）を受け取り、S902でその受け取ったデータを保管、あるいはWebなどに公開する。その際、預託公開署名記録には識別のための固有の公開ID（項目1003）を付与する。預託公開署名記録は公開IDとともに公開署名記録保管領域818に保管される。

【0060】

S902により、公開機関側装置104は、公開したデータ（預託公開署名記録）について、S903で、ユーザ名（項目1002）、公開ID（項目1003）、預託公開署名記録の署名番号（項目302、項目1004）、公開日（項目1006）、公開場所（あるいは保管場所）（項目1005）を、公開機関側装置104の公開データベース814に登録する。

【0061】

公開データベースの構成例を図10に示す。公開データベースには、ユーザごとに公開ID1003、公開した預託公開署名記録の署名番号1004（図3の302に相当）、公開場所1005、公開日1006が記録され、この公開データベースを参照することによって、どのユーザのどのような情報をいつどこに公開したかを知ることができる。

【0062】

その後、S904で、公開機関側装置104は、公開通知依頼データベース815を参照し、今回の公開に関わるユーザについて、他のユーザから公開通知依頼があるかどうか調べ、ある場合は、S905で公開通知処理（S1203、S1204）を行う。公開通知依頼データベース815の詳細および、公開通知処理の詳細は、後述の公開通知サービスの説明のところで述べる。

【0063】

S904で、公開機関側装置104は、今回の公開に関わるユーザについて、他のユーザから公開通知依頼が無ければ、S906に進む。

【0064】

S906では、公開機関側装置104は、公開データを受け取り正常に公開した旨を公開依頼ユーザに伝える文書を作成し、公開依頼ユーザに送信する。

【0065】

公開催促サービス702は、一定期間公開が無いユーザに対して、公開機関側装置104が公開を催促するサービスである。これにより、ユーザ側における公開忘れを防止し、預託公開署名記録が無いために連鎖検証が困難となるといった状況を防ぐ。

【0066】

公開催促処理の流れを図11に示す。

【0067】

公開機関側装置104は、公開催促サービス702を行う際、公開催促プログラム810により、以下のS1101～S1104の公開催促処理を行う。

【0068】

S1101において、公開機関側装置104は、S903で預託公開署名記録が登録された公開データベース1001の各ユーザの最新の公開データに対して、項目「公開日」（1006）および項目「催促日」（1007）を参照し、一定期間（例えば、一ヶ月）経過しているものについて、ユーザ名を抽出する。

【0069】

図10の例では、現在日時が2003年9月10日であるとする、各ユーザの最新の公開データ（レコード1009、1010、1012、1015）のうち、レコード1009、1015は前回の公開から一ヶ月以上経過しており、レコード1012は、前回の催促日から一ヶ月以上経過しているので、それぞれのレコードの項目「ユーザ名」（1002）からユーザA、ユーザC、ユーザDが抽出される。

【0070】

S1102において、公開機関側装置104は、S1101で抽出したユーザに送信する

ための公開催促書706（公開を催促する文書）を作成し、S1103で、その公開催促書を送信する。ユーザ名と送信先（メールアドレスなど）の対応付けは、上記データベース1001に新たに項目を追加して送信先を記録することによって行っても良いし、ユーザ名と送信先（メールアドレスなど）を対応付けるためのデータベースを別に作成することによって行っても良い。

【0071】

最後に、S1104において、公開機関側装置104は、公開催促書を送信したことを記録するために、催促したユーザについて、催促対象となった各ユーザの最新のレコードの項目「催促日」（1007）に公開催促書送信日を記録する。

【0072】

公開通知サービス703は、公開通知依頼707に従って、あるユーザに関わる公開が行われたことを、公開機関側装置104が公開通知708によって、別のユーザに通知するサービスである。検証者側装置は、署名者側装置の預託公開署名記録が公開されたことを公開機関側装置104より通知してもらうことによって、検証対象署名が署名者側装置の署名履歴を用いて連鎖検証することが可能となったことを知ることができる。

【0073】

公開通知処理の流れを図12に示す。

【0074】

公開機関側装置104は、公開通知サービス703を行う際、公開通知プログラム811の実行により、以下のS1201～S1204の公開通知処理を行う。

【0075】

S1201で、公開機関側装置104は、ユーザAより「ユーザBに関わる預託公開署名記録が次に公開された時、連絡下さい」との公開通知依頼書を受け取ると、公開機関側装置104はS1202で、その公開通知依頼内容を公開通知依頼データベース815に登録する。

【0076】

公開通知依頼データベース1301（図8の815）の構成を図13に示す。公開通知依頼データベース1301には、公開通知の対象となる公開者「被依頼ユーザ名」（1302）、公開通知依頼者情報「公開依頼ユーザ名（メールアドレス）」（1303）、公開通知依頼日を表す「依頼日」（1304）、公開通知済であるか否かを表す「通知有無」（1305）を登録する。上記例では、被依頼ユーザ名は「ユーザB」、公開通知依頼ユーザ名は「ユーザA」となる。

【0077】

図9の公開処理において、S904で、公開機関側装置104は、公開通知依頼データベース1301を参照し、今回公開した公開署名記録に対して、他のユーザから公開通知依頼があるかどうか調べ、ある場合は、以下の通知書送信処理を行う。

【0078】

まず、S1203で、公開機関側装置104は、今回の公開（預託公開署名記録の公開を依頼したユーザ側装置に関わる公開）について通知を依頼したユーザを抽出する。例えば、今回の公開者がユーザBである場合、公開通知依頼データベースの項目「被依頼ユーザ名」（1302）がユーザBであるレコード1306の項目「依頼ユーザ名」（1303）より、ユーザAが抽出される。

【0079】

S1204で、公開機関側装置104は、S1203で抽出したレコードの項目「通知有無」（1305）が「未」であれば、S1203で抽出したユーザに対して公開通知書708を送信する。送信後、S1203で抽出したレコードの項目「通知有無」（1305）に送信日を記録する。

【0080】

検証代行サービス704は、ユーザ（検証者）側装置に代わって、公開機関側装置104が署名の検証を行うサービスである。検証に必要な署名者側装置の署名履歴や預託公開

署名記録の収集といった検証者の手間を減らすことができる。また、公的な第三者機関側装置である公開機関側装置 104 が、検証結果を前述の検証ログとして公開することで、署名の有効性をより高い信頼性で保証するとともに、長期に渡って検証結果を保証することができる。公開された検証ログには、検証に利用したデータが記載されているので、公開機関側装置 104 に限らず誰でもその内容を再検証することが可能である。

【0081】

検証代行サービス 704 は、検証代行依頼書受信処理と署名検証処理の2つに分けられる。検証代行依頼書受信処理の流れを図 14 に、署名検証処理の流れを図 15 に示す。

【0082】

公開機関側装置 104 は、検証代行サービス 704 を行う際、検証代行プログラム 812 により、以下の S1401～S1406 の検証代行依頼書受信処理、および S1501～S1508 の署名検証処理を行う。

【0083】

S1401 で公開機関側装置 104 は、検証者側装置より検証代行依頼書 709 を受け取る。検証代行依頼書には、検証対象署名付き文書、署名者名（メールアドレス）、検証代行依頼者名（メールアドレス）が記載されている。

【0084】

S1402 で、公開機関側装置 104 は、S1401 で受け取った検証代行依頼書に対し、固有の検証IDを付与する。検証IDが付けられた検証代行依頼書は、検証代行依頼書保管領域 819 に保管する。

【0085】

S1403 において、公開機関側装置 104 は、検証対象署名の署名番号（項目 302）以降で、検証対象署名の署名者側装置により公開を預託された公開データ（預託公開署名記録（図 5 の 513 に相当））があるかどうか、公開データベース 1001 の項目「ユーザ名」（1002）および項目「署名番号」（1004（図 3 の 302 に相当））により調べる。具体的には、検証対象署名の署名者と同じユーザ名を持つレコードを抽出し、抽出したレコードに対して、項目「署名番号」（1004（図 3 の 302 に相当））を調べ、検証対象署名の署名番号より大きくかつ直近の署名番号を持つレコードを抽出する。目的の公開データが無い場合は、S1406 に進む。

【0086】

S1404 において、公開機関側装置 104 は、検証対象署名が検証できるような署名履歴が署名履歴保管領域 817 に存在するかどうかが調べる。具体的には、検証対象署名の署名者側装置の署名履歴であり、かつ検証対象署名の署名番号から S1403 で抽出したレコードの署名番号までの範囲を含んでいる署名履歴が、署名履歴保管領域に存在しているか調べる。既に存在していれば、S1406 に進み、存在していなければ、S1405 において、検証対象署名の署名者側装置に対し、検証対象署名の署名番号から S1403 で抽出したレコードの署名番号までの範囲を含んでいる署名履歴の送付を要請する。

【0087】

S1406 で、公開機関側装置 104 は、現段階の検証状況を検証状況データベースに記録する。

【0088】

検証状況データベース 1601（図 8 の 816）の構成を図 16 に示す。検証状況データベース 1601 には、S1402 で生成した「検証ID」（1602）、検証代行依頼者を表す「依頼ユーザ名」（1603）、検証対象署名の署名者を表す「検証対象署名者」（1604）、検証に利用する公開書名記録の公開IDを示す「公開ID」（1605）、検証依頼日を示す「依頼日」（1606）、検証状況を示す「検証状況」（1607）が記録される。検証ID 1602 は、検証代行依頼書と検証状況データベースのレコードとを対応付ける。また、検証状況 1607 には、S1403 で預託公開署名記録が存在していなかったことを示す「公開記録無」、S1404 で署名履歴が存在していたことを示す「履歴取得済」、S1404 で署名履歴が存在しておらず、署名履歴を検証対象署名の署名者

側装置に要請中であることを示す「履歴取得中」、既に検証が終了していることを示す「検証完了」といった情報が記録される。

【0089】

検証代行依頼書受信処理が終了した検証代行依頼については、次の署名検証処理を行う。

【0090】

署名検証処理を行うタイミングとしては、検証代行依頼書受信処理が終了した直後、あるいは、1日おきなど一定間隔、あるいは、S1405で要請した署名履歴が、ユーザより送付され、履歴受信プログラム813により、受け取った署名履歴が署名履歴保管領域817に保存された時などがある。

【0091】

公開機関側装置104の履歴受信プログラム813は、受け取った署名履歴および送信者名を署名履歴保管領域817に保存するとともに、検証状況データベース1601の該当するレコードの項目「検証状況」(1607)に「履歴取得済」を記録する。該当するレコードとは、検証状況データベース1601の項目「検証対象署名者」(1604)と署名履歴送信者が同じであり、かつ項目「検証ID」(1602)に対応する検証代行依頼書(検証代行依頼書保管領域に保管されている)の検証対象署名の署名番号から項目「公開ID」(1605)に対応する預託公開署名記録(公開署名記録保管領域に保管されている)の署名番号までの範囲が履歴受信プログラムで受信した署名履歴に含まれているレコードである。

【0092】

署名検証処理においては、まず、S1501で、公開機関側装置104は、検証状況データベース1601において、今から検証を行う検証代行依頼書について、検証ID1602を参照して該当するレコード(検証IDが検証代行依頼書の検証IDと一致するレコード。検証対象レコードと呼ぶ)を抽出し、検証状況1607を確認する。検証代行依頼書に添付されている署名(ユーザが検証を依頼した署名)を以降、検証対象署名と呼ぶ。

【0093】

S1501において、検証状況1607が、「公開記録無」の場合は、S1506へと進み、公開機関側装置104は、検証代行依頼書の検証対象署名の署名番号(項目402)以降で、検証対象署名の署名者側装置により公開を預託された預託公開署名記録があるかどうか、公開データベース1001の項目「ユーザ名」(1002)および項目「署名番号」(1004)により調べる。具体的には、検証対象署名の署名者と同じユーザ名を持つレコードを抽出し、抽出したレコードに対して、項目「署名番号」(1004)を調べ、検証対象署名の署名番号より大きくかつ直近の署名番号を持つレコードを抽出する。目的の預託公開署名記録が無い場合は、署名検証処理を終了する。

【0094】

S1506で、検証対象署名の署名者側装置の該当する預託公開署名記録があった場合、公開機関側装置104は、S1507において、検証対象署名が検証できるような署名履歴が署名履歴保管領域817に存在するかどうか調べる。具体的には、検証対象署名の署名者側装置の署名履歴であり、かつ検証対象署名の署名番号からS1506で抽出したレコードの署名番号までの範囲を含んでいる署名履歴が、署名履歴保管領域に存在しているか調べる。

【0095】

既に存在していれば、S1502に進む。存在していなければ、S1508において、検証対象署名の署名者側装置に対し、検証対象署名の署名番号からS1506で抽出したレコードの署名番号までの範囲を含んでいる署名履歴の送付を要請し、S1504に進む。S1504では、公開機関側装置104は、検証状況データベース1601において、検証対象の検証代行依頼書について、検証ID1602を参照して検証IDが検証代行依頼書の検証IDと一致するレコードを抽出し、検証状況1607に「履歴取得中」を記録して、署名検証処理を終了する。

【0096】

S1501において、検証状況1607が、「履歴取得中」の場合は、S1505へと進み、公開機関側装置104は、検証対象署名が検証できるような署名履歴が署名履歴保管領域817に存在するかどうか調べる。具体的には、検証対象署名の署名者側装置の署名履歴であり、かつ検証対象署名の署名番号から検証対象署名の署名者側装置の預託公開署名記録の署名番号までの範囲を含んでいる署名履歴が、署名履歴保管領域に存在しているか調べる。

【0097】

ここで、検証対象署名の署名者側装置の預託公開署名記録の署名番号は、次のようにして求める。まず、検証対象の検証代行依頼書の検証IDを取得し、検証状況データベース1601において、検証ID1602を参照して該当するレコード（検証IDが検証代行依頼書の検証IDと一致するレコード）を抽出する。抽出したレコードにおいて、公開ID1605を取得する。

【0098】

次に、公開データベース1001において、公開ID1003を参照して該当するレコード（公開IDが検証状況データベースより抽出したレコードの公開ID1605と一致するレコード）を抽出し、そのレコードの署名番号1004を取得する。この署名番号が、検証対象署名の署名者側装置の預託公開署名記録の署名番号である。検証対象署名が検証できるような署名履歴が署名履歴保管領域817に存在していれば、S1502に進み、存在していなければ、署名検証処理を終了する。

【0099】

S1501において、検証状況1607が「履歴取得済」である場合は、S1502へと進む。

【0100】

S1501において、検証状況1607が「検証完了」である場合は、署名検証処理を終了する。

【0101】

S1502では、公開機関側装置104は、検証代行依頼書より検証対象署名501（図3の310に相当）を取得し、S1501で抽出した検証対象レコードの項目「検証対象署名者」（1604）の署名履歴であり、かつ検証対象署名の署名番号から検証対象署名の署名者側装置の預託公開署名記録の署名番号までの範囲を含んでいる署名履歴を取得する。

【0102】

ここで、検証対象署名の署名者側装置の預託公開署名記録の署名番号は、次のようにして求める。まず、検証対象の検証代行依頼書の検証IDを取得し、検証状況データベース1601において、検証ID1602を参照して該当するレコード（検証IDが検証代行依頼書の検証IDと一致するレコード）を抽出する。抽出したレコードにおいて、公開ID1605を取得する。

【0103】

次に、公開データベース1001において、公開ID1003を参照して該当するレコード（公開IDが検証状況データベースより抽出したレコードの公開ID1605と一致するレコード）を抽出し、そのレコードの署名番号1004を取得する。この署名番号が、検証対象署名の署名者側装置の預託公開署名記録の署名番号である。

【0104】

また、検証対象レコード中の公開ID1605に対応する預託公開署名記録513を公開署名記録保管領域より取得する。そして、以上取得したデータの検証対象署名501（図3の310に相当）、検証対象署名の署名者側装置の署名履歴502、検証対象署名の署名者側装置の預託公開署名記録513、公開機関側装置104の署名履歴517、新聞公開署名記録526を用いて、図5のS527、S528、S529の処理を行い、検証対象署名を検証する。

【0105】

S1503において、S1502での検証に利用したデータ「検証対象署名501（図3の310に相当）」「署名履歴502（署名記録503、507～509）」「預託公開署名記録513」「公開機関側装置104の署名履歴517」「新聞公開署名記録526」を記録した検証ログを作成し、検証対象レコードの項目「依頼ユーザ名（メールアドレス）」（1603）を参照して検証代行依頼ユーザに、作成した検証ログ710（図6の601に相当）を送信する。

【0106】

最後に、S1504において、検証対象レコードの項目「検証状況」（1607）に「検証完了」を記録する。

【0107】

また、署名検証処理終了後、検証状況データベース中の項目「依頼日」（1606）を参照して、一定期間が経過しているにもかかわらず検証状況が「検証完了」になっていないレコードを抽出し、そのレコードに該当する検証代行依頼書については、検証できなかった旨を伝える文書を検証代行依頼者1603に送信する。

【0108】

ここで、以下のような状況における本実施形態における検証代行の流れを図17を用いて述べる。

【0109】

今、ユーザB側装置は、ユーザA側装置よりAのヒステリシス署名付き契約書（有効期間5年間）1701を3ヶ月前に受信したとする。ヒステリシス署名は、長期証拠性を維持する署名技術であるが、ユーザA側装置の作成した署名を検証するためには、ユーザA側装置がきちんと署名履歴を保管しておく必要があり、契約書の証拠性は、ユーザA側装置の署名履歴保持に依存している。このような場合、契約書の証拠性を高めるためにユーザB側装置は、公開機関側装置104に検証代行を依頼し、検証ログを発行してもらうことができる。

【0110】

まず、ユーザB側装置は、ユーザA側装置のヒステリシス署名付き契約書（以降、検証対象署名と呼ぶ。署名番号は「10」）を添付した検証代行依頼書1702（図7の709に相当）を作成し、公開機関側装置104に送信する。

【0111】

ユーザB側装置より検証代行依頼書1702（図7の709に相当）を受け取った公開機関側装置104は、検証代行プログラム812の処理により、図14、図15の検証代行処理を行う。S1401で受け取った検証代行依頼書1702（図7の709に相当）に対して、S1402で検証IDを作成する。本例では、検証ID「000001」が作成された。検証代行依頼書1702（図7の709に相当）は、検証ID「000001」とともに、公開機関側装置104の検証代行依頼書保管領域819に保管される。

【0112】

公開機関側装置104では、S1403において、検証対象署名の署名番号（「10」）以降で、検証対象署名の署名者ユーザA側装置により公開を預託された預託公開署名記録があるかどうか、公開データベース1001の項目「ユーザ名」（1002）および項目「署名番号」（1004）により調べる。その結果、レコード1009は、項目「ユーザ名」が「ユーザA」であり、項目「署名番号」が「32」で検証対象署名の署名番号「10」より大きいので、該当するレコードである。

【0113】

S1404において、公開機関側装置104は、検証対象署名の署名者「ユーザA」の署名履歴であり、かつ検証対象署名の署名番号「10」からS1403で抽出したレコードの署名番号「32」までの範囲を含んでいる署名履歴が、公開機関側装置104の署名履歴保管領域817に存在しているか調べる。本例では、存在していなかったため、S1405において、公開機関側装置104は、検証対象署名の署名者「ユーザA」に対し、検

証対象署名の署名番号「10」からS1403で抽出したレコードの署名番号「32」までの範囲を含んでいる署名履歴の送付を要請する。

【0114】

S1406で、公開機関側装置104は、現段階の検証状況を検証状況データベース1601に記録して、検証代行依頼書受信処理を終了する。本例について記録したものがレコード1608である。「検証ID」(=000001)、「依頼ユーザ名」(=ユーザB)、「検証対象署名者」(=ユーザA)、「公開ID」(=000142)、「依頼日」(=2003年9月10日)、「検証状況」(=履歴取得中)である。

【0115】

署名履歴の送付を要請していたユーザA側装置より署名履歴が送られてきたら、公開機関側装置104は、履歴受信プログラム813により、受け取ったユーザA側装置の署名履歴および送信者名「ユーザA」を署名履歴保管領域817に保存するとともに、検証状況データベース1601の項目「検証対象署名者」(1604)について署名履歴送信者「ユーザA」と同じであるレコード1608を抽出する。

【0116】

次に、レコード1608の項目「検証ID」(=000001)に対応する検証代行依頼書1702(図7の709に相当)(検証代行依頼書保管領域に保管されている)を調べ、添付されている検証対象署名の署名番号「10」からレコード1608の項目「公開ID」(=000142)に対応する預託公開署名記録(公開署名記録保管領域に保管されている)の署名番号「32」までの範囲が履歴受信プログラムで受信した署名履歴に含まれていれば、検証状況データベース1601のレコード1608の項目「検証状況」に「履歴取得済」を記録する。

【0117】

検証に必要な署名履歴が取得されたタイミングで、公開機関側装置104は、上記レコード1608の検証依頼(検証ID「000001」の検証代行依頼書1702(図7の709に相当))について、以下の署名検証処理を行う。本例では、このタイミングとしたが、定期的に全レコードに対して署名検証処理を行っても良い。

【0118】

署名検証処理においては、まず、S1501で、公開機関側装置104は、検証状況データベース1601において、今から検証を行う検証代行依頼書1702(図7の709に相当)と同じ検証ID「000001」を持つレコード1608を抽出し、検証状況を確認する。検証状況1607が「履歴取得済」であるので、S1502へと進む。

【0119】

S1502では、公開機関側装置104は、検証代行依頼書1702(図7の709に相当)より検証対象署名付き文書1701を取得し、S1501で抽出したレコード1608の項目「検証対象署名者」(=「ユーザA」)の署名履歴であり、かつ「検証対象署名の署名番号」(=「10」)からレコード1608の公開ID(=「000142」)に対応する「預託公開署名記録の署名番号」(=「32」)までの範囲を含んでいる署名履歴を公開機関側装置104の署名履歴保管領域817より取得する。

【0120】

また、レコード1608の公開ID(=「000142」)に対応する預託公開署名記録を公開署名記録保管領域818より取得する。そして、検証対象署名と上記取得した署名履歴、預託公開署名記録、公開機関側装置104の署名履歴、新聞公開署名記録を用いて、図5のS527、S528、S529の処理を行い、検証対象署名を検証する。

【0121】

S1503において、公開機関側装置104は、S1502での検証に利用したデータ「検証対象署名」「署名者側装置の署名履歴」「預託公開署名記録」「公開機関側装置104の署名履歴」「新聞公開署名記録」を記録した検証ログ(601)を作成し、レコード1608の項目「依頼ユーザ名(メールアドレス)」(=「ユーザB」)を参照して検証代行依頼ユーザ「ユーザB」側装置に作成した検証ログ1703(図6の601、図7の

710に相当)を送信する。

【0122】

最後に、公開機関側装置104は、S1504において、レコード1608の項目「検証状況」に「検証完了」を記録する。

【0123】

以上の公開機関側装置104の検証代行サービスにより、ユーザAの契約書に対する検証ログ1703(図6の601、図7の710に相当)を受け取ったユーザB側装置は、検証ログに記載されている検証対象署名がユーザA側装置から受け取った契約書の署名と一致していること、また、公開機関側装置104のHPなどを参照し、検証ログに記載されている預託公開署名記録が公開機関側装置104によって公開されているものと一致していること、あるいは検証ログに記載されている新聞公開署名記録が新聞に掲載されている新聞公開署名記録と一致していることを確認する。

【0124】

そして、それらが確認できた検証ログをユーザB側装置の検証ログ保管領域217に保管しておく、または公開機関側装置104の検証ログ保管領域820に保管しておくことによって、ユーザB側装置は、ユーザA側装置に頼らず、いつでも自身の保管する検証ログによって署名の正当性を示すことができる。

【図面の簡単な説明】

【0125】

【図1】第1実施形態が適用されたシステムの概略図である。

【図2】第1実施形態におけるユーザ側装置の構成図である。

【図3】ヒステリシス署名技術の概略図である。

【図4】公開機関側装置の公開の仕組みを表した図である。

【図5】検証ログ作成を含む連鎖検証手順を説明するためのフロー図および概念図である。

【図6】検証ログの内容を表した図である。

【図7】本実施形態における公開機関側装置のサービス形態を表した図である。

【図8】本実施形態における公開機関側装置の構成図である。

【図9】公開機関側装置の公開処理のフロー図である。

【図10】公開機関側装置の公開データベースを表した図である。

【図11】公開機関側装置の公開催促処理のフロー図である。

【図12】公開機関側装置の公開通知処理のフロー図である。

【図13】公開機関側装置の公開通知依頼データベースを表した図である。

【図14】公開機関側装置の検証代行処理のうち、検証代行依頼書受信処理のフロー図である。

【図15】公開機関側装置の検証代行処理のうち、署名検証処理のフロー図である。

【図16】公開機関側装置の検証状況データベースを表した図である。

【図17】検証代行の例を表した図である。

【符号の説明】

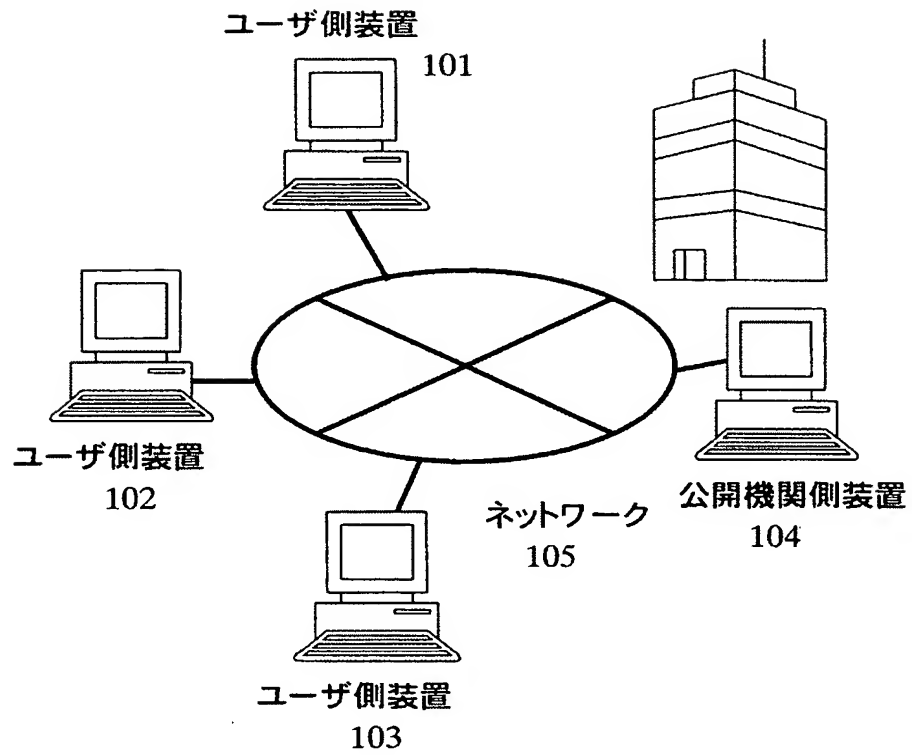
【0126】

101~103:ユーザ側装置、104:公開機関側装置、105:ネットワーク、301:項目(「識別番号」)、302:項目(「署名番号」)、303:項目(「種別」)、304:項目(「前回署名記録のハッシュ値」)、305:項目(「文書のハッシュ値」)、306:項目(「署名 or 受信署名記録情報」)、307:送信文書、308、310:署名、309:受信文書、311:署名履歴、312~315:署名記録、401:項目(「識別番号」)、402:項目(「署名番号」)、403:項目(「前回署名記録のハッシュ値」)、404:項目(「署名値」)、405:項目(「公開ID」)、406:項目(「預託公開署名記録番号」)、407:項目(「預託公開署名記録のハッシュ値」)、408:公開依頼書、409:署名、410:公開機関側装置の署名履歴、411~413:署名記録、501:検証対象署名付き文書、502:署名履歴、503~

509:署名記録、504、510:項目(「署名番号」)、505、511:項目(「前回署名記録のハッシュ値」)、506、512:項目(「署名値」)、513:預託公開署名記録、514:預託公開署名記録の項目(「署名番号」)、515:預託公開署名記録の項目(「前回署名記録のハッシュ値」)、516:預託公開署名記録の項目(「署名値」)、517:公開機関側装置の署名履歴、518、523、524:公開機関側装置の署名記録、519:項目(「署名番号」)、520、525:項目(「前回署名記録のハッシュ値」)、521:項目(「公開ID」)、522:項目(「預託公開署名記録のハッシュ値」)、526:新聞公開署名記録、601:検証ログ、602:項目(「作成日」)、603:項目(「検証署名」)、604~607:項目(「署名履歴」)、608:項目(「預託公開署名記録」)、609:項目(「公開場所」)、610~612:項目(「公開機関側装置の署名履歴」)、613:項目(「新聞公開署名記録」)、614:項目(「新聞公開先」)、615:項目(「公開鍵」)、701:公開サービス、702:公開催促サービス、703:公開通知サービス、704:検証代行サービス、705:公開を依頼する署名記録、706:公開催促書、707:公開通知依頼書、708:公開通知書、709:検証代行依頼書、710:検証ログ、1001:公開データベース、1002:項目(「ユーザ名」)、1003:項目(「公開ID」)、1004:項目(「署名番号」)、1005:項目(「公開場所」)、1006:項目(「公開日」)、1007:項目(「催促日」)、1008~1015:公開データベースのレコード、1301:公開通知依頼データベース、1302:項目(「被依頼ユーザ名」)、1303:項目(「依頼ユーザ名」)、1304:項目(「依頼日」)、1305:項目(「通知有無」)、1306~1308:公開通知依頼データベースのレコード、1601:検証状況データベース、1602:項目(「検証ID」)、1603:項目(「依頼ユーザ名」)、1604:項目(「検証対象署名者」)、1605:項目(「公開ID」)、1606:項目(「依頼日」)、1607:項目(「検証状況」)、1608~1611:検証状況データベースのレコード、1701:検証対象署名付き文書、1702:検証代行依頼書、1703:検証ログ

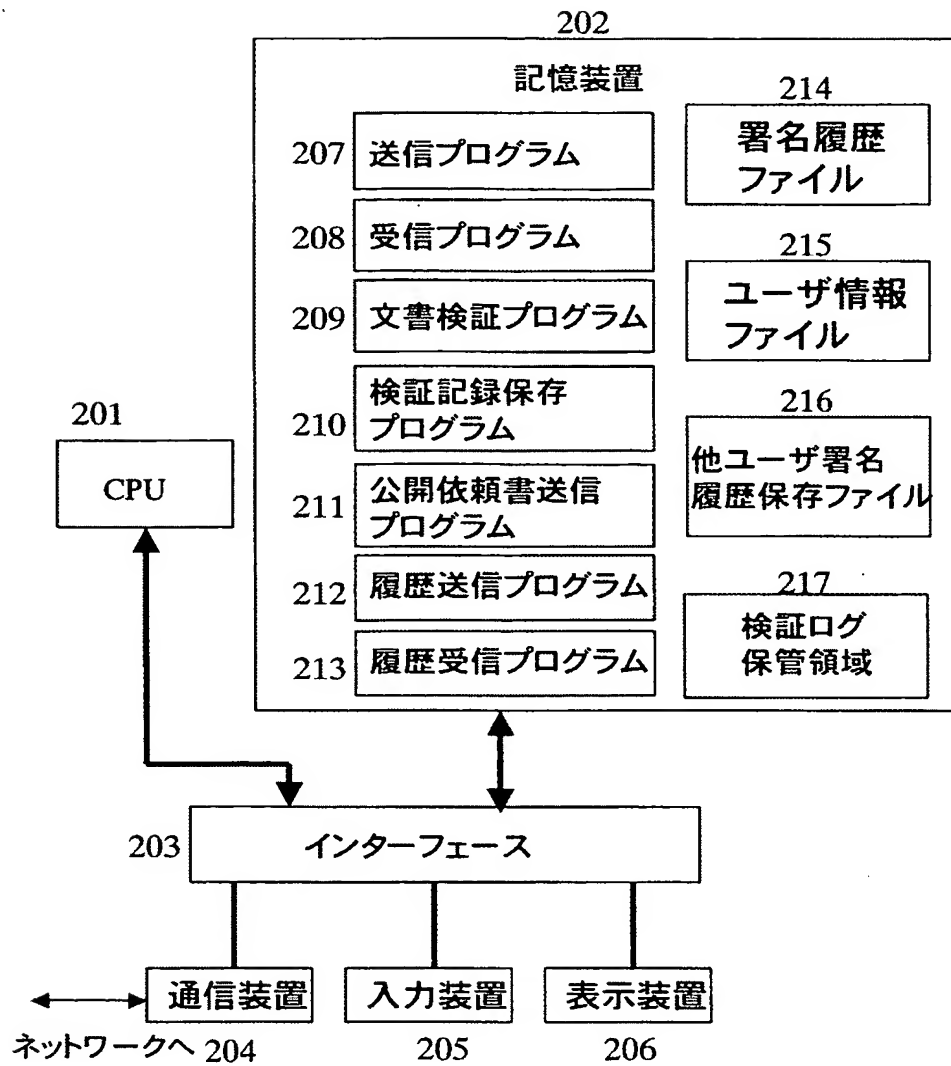
【書類名】 図面
【図 1】

【図 1】



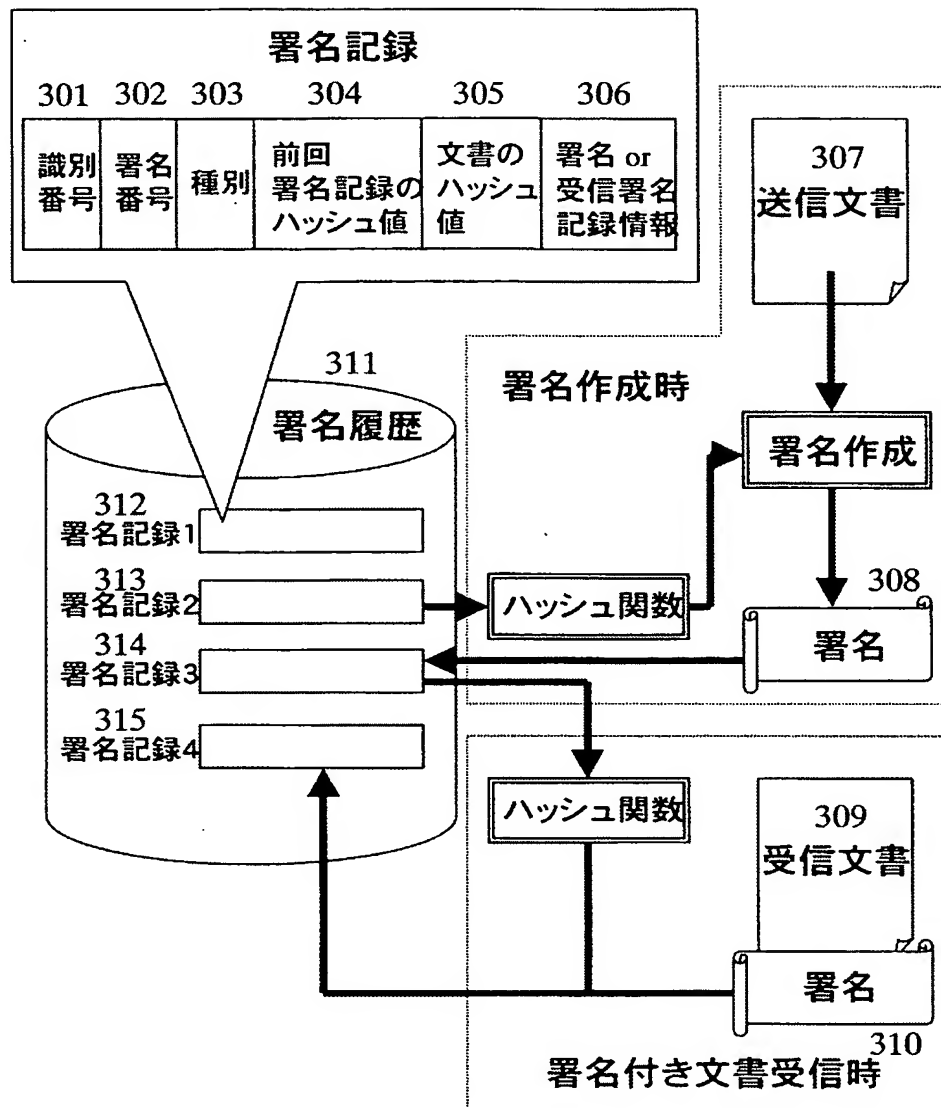
【図2】

【図2】



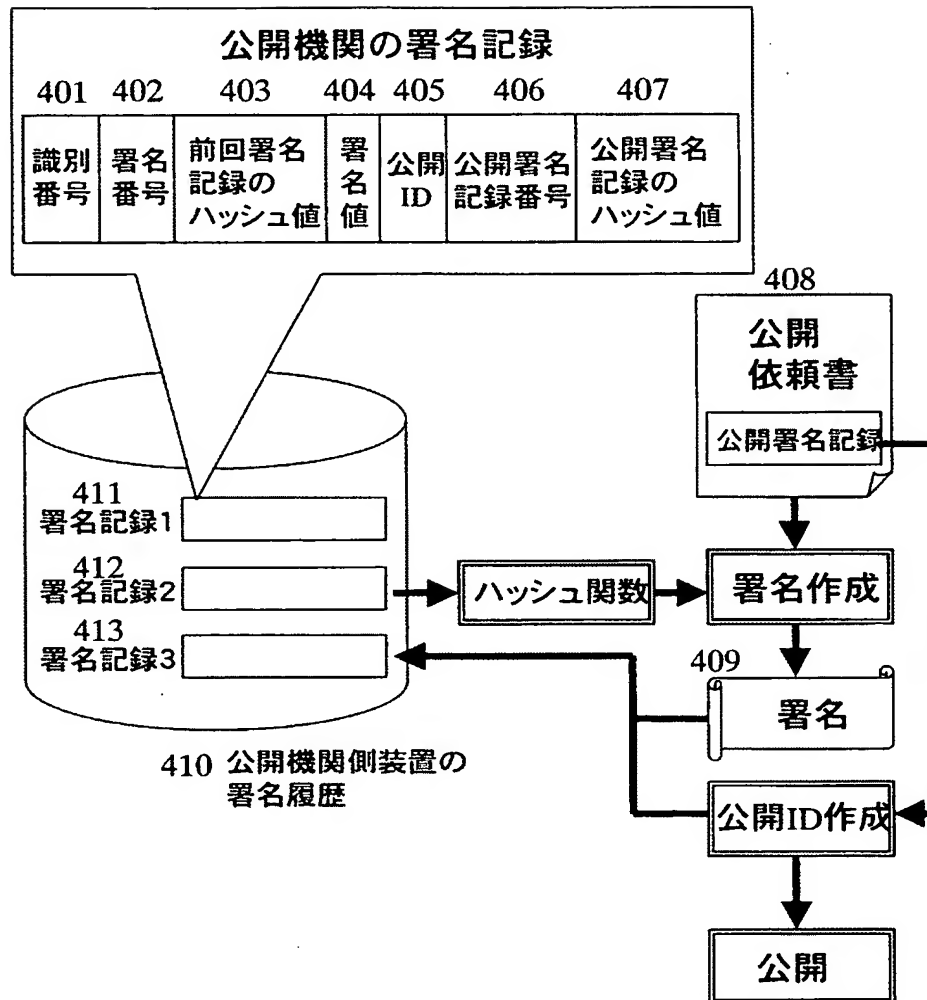
【図3】

【図3】



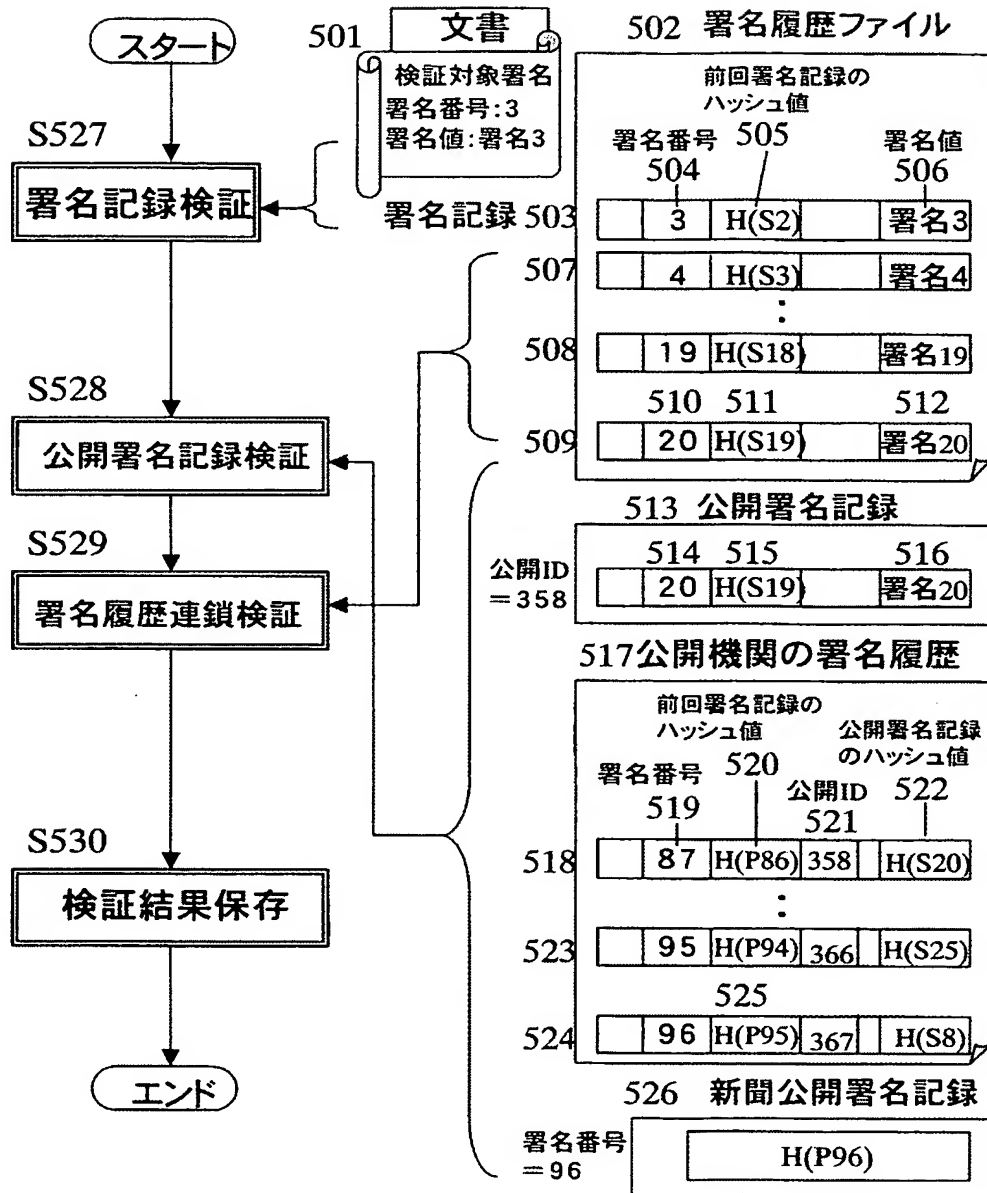
【図4】

【図4】



【図5】

【図5】



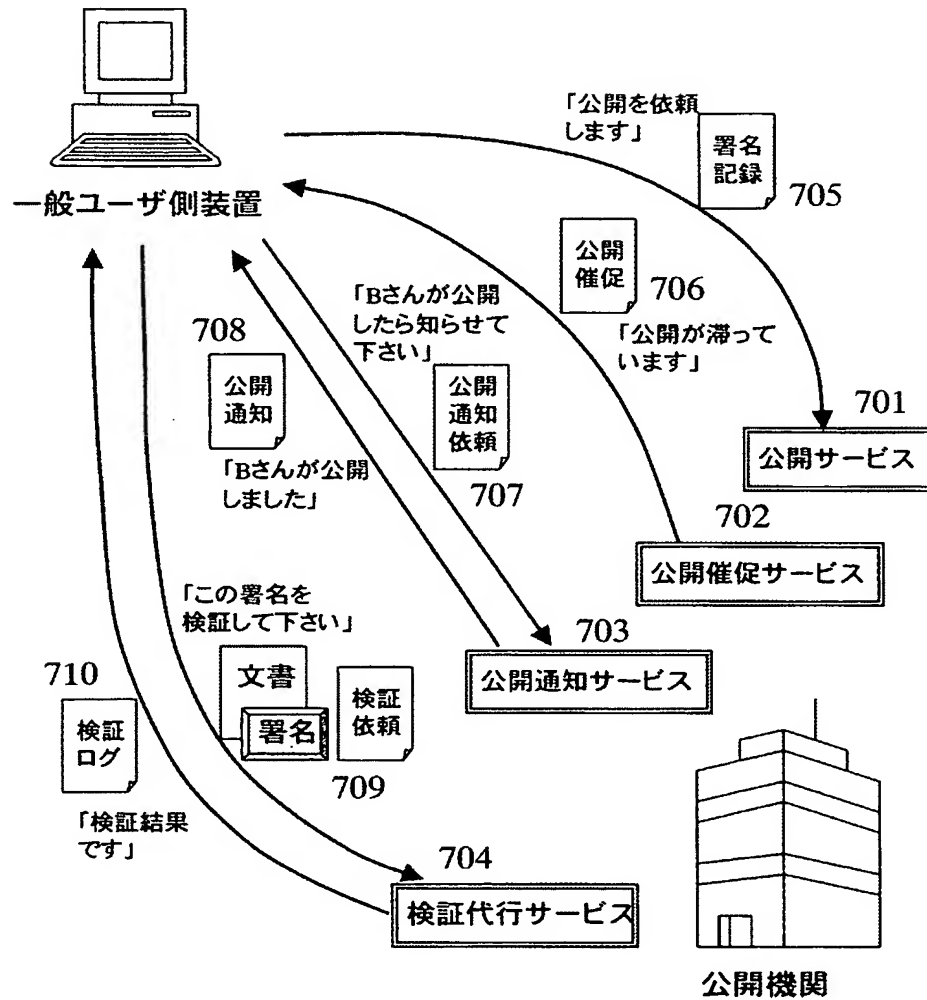
【図6】

【図6】

601	検証ログ	
602	作成日: 2003年8月29日	
	検証署名:	
603	01063A78BA216574EC5F77F3315	
	署名履歴:	
604	01063A78BA21657499002DEC5F77F3315	
605	01074D830A03B187E3FF22289BAC09121	
606	01089BBA21865740BE7F21FE339647381	
607	0109E324876529C1D36FA119503645B193	
	公開署名記録: 公開ID= 377	
608	0109E324876529C1D36FA119503645B193	
	609 公開場所 (http://www.XXX.co.jp/)	
	公開機関の署名履歴:	
610	011084FA2195859449946372900BC21543	
611	01114563B281AEE7E3FF2229DC2190031	
612	01124A849035462CD18593404093672874	
	新聞公開署名記録: 署名番号= 112	
613	01124A849035462CD18593404093672874	
	614 ○○新聞社2003年9月10日朝刊	
	公開鍵:	
615	C7A437BA93739102937577476483CA128	

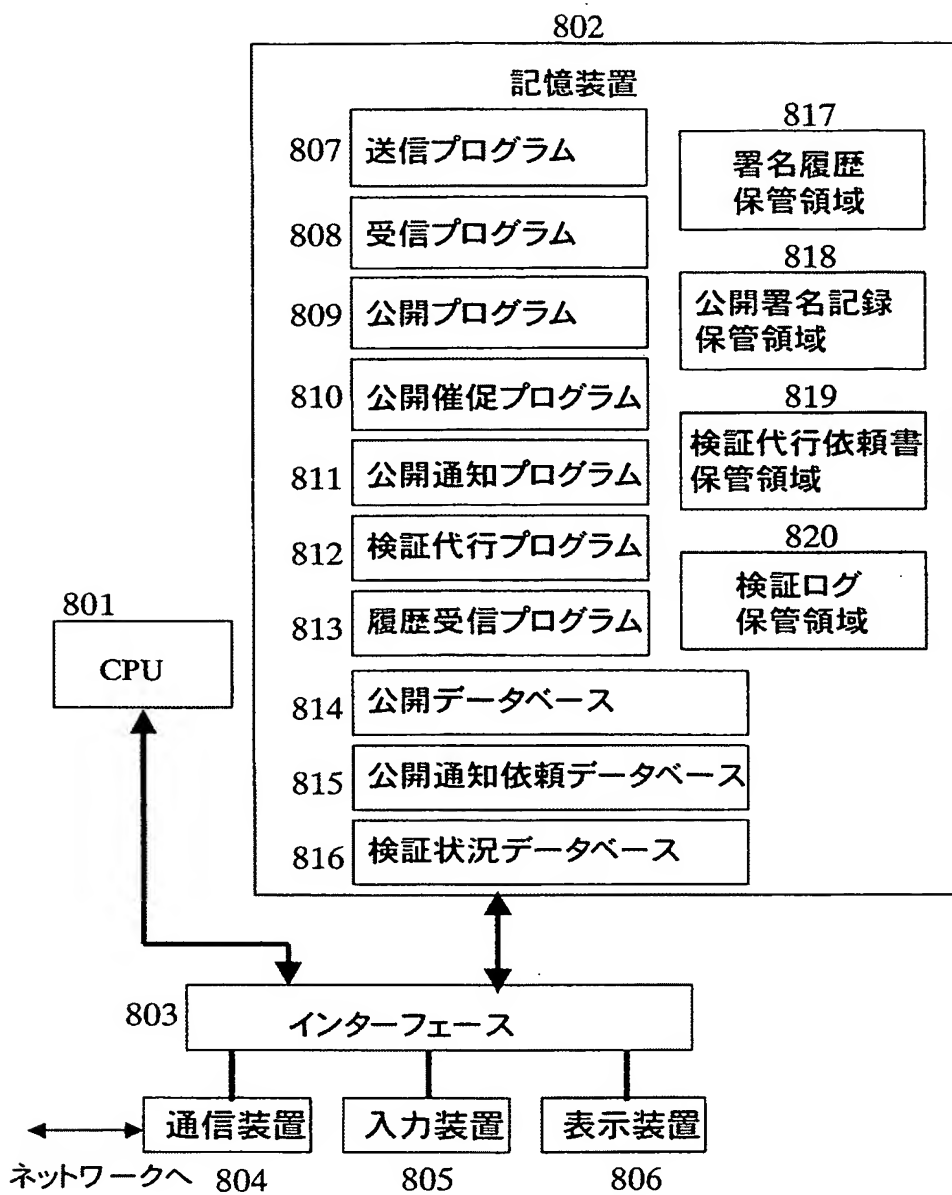
【図 7】

【図 7】



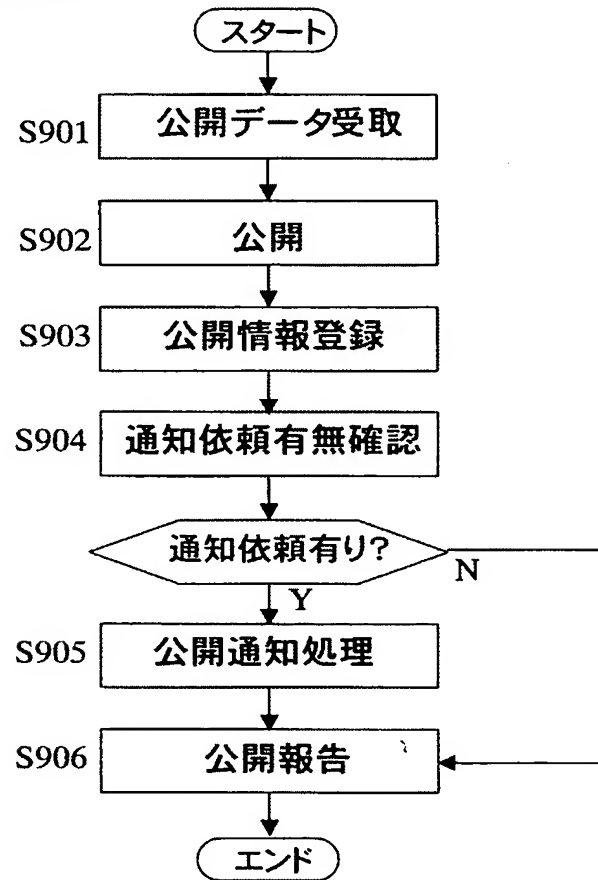
【図 8】

【図 8】



【図9】

【図9】

公開処理

【図10】

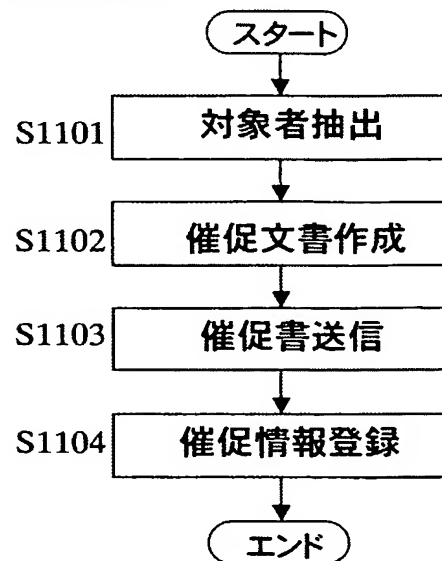
【図10】

1001 公開データベース

1002	1003	1004	1005	1006	1007	
ユーザ名	公開ID	署名番号	公開場所	公開日	催促日	
ユーザA	000125	000002	http://www.X.co.jp/	2003.0710	—	1008
	000142	000032	http://www.X.co.jp/	2003.0802	—	1009
ユーザB	000225	000004	http://www.X.co.jp/	2003.0909	—	1010
ユーザC	000003	000003	http://www.X.co.jp/	2002.1104	2003.0618	1011
	000099	000155	http://www.X.co.jp/	2003.0620	2003.0729	1012
ユーザD	000090	000002	http://www.X.co.jp/	2003.0615	—	1013
	000118	000055	http://www.X.co.jp/	2003.0705	2003.0807	1014
	000148	000106	http://www.X.co.jp/	2003.0808	—	1015

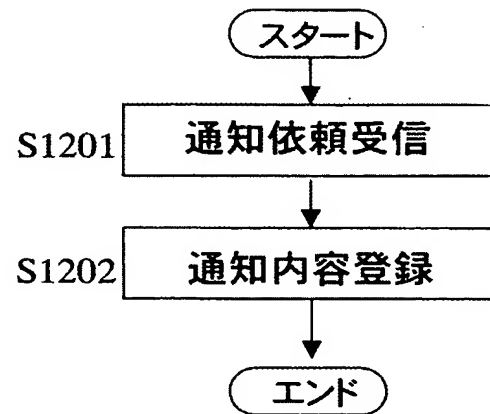
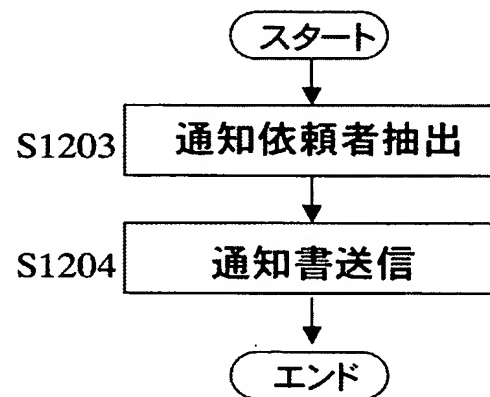
【図11】

【図11】

公開催促処理

【図12】

【図12】

公開通知処理<通知依頼受信処理><通知書送信処理>

【図13】

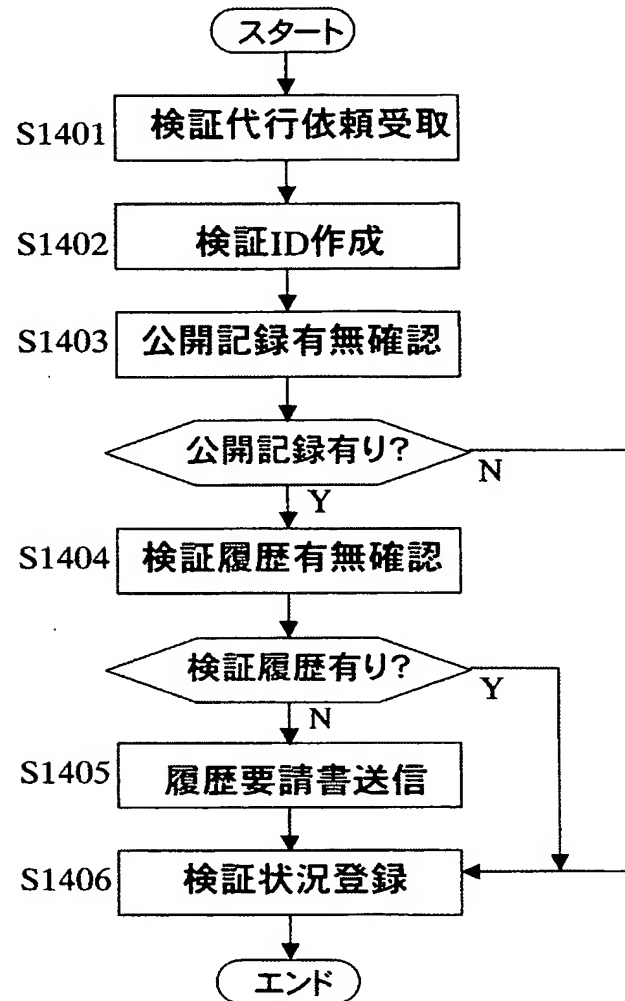
【図13】

1301 公開通知依頼データベース

1302	1303	1304	1305	
被依頼ユーザ名	依頼ユーザ名 (メールアドレス)	依頼日	通知有無	
ユーザB	ユーザA (ユーザA@XX.co.jp)	2003.0710	未	1306
ユーザD	ユーザC (ユーザC@YY.co.jp)	2003.0511	2003.0522	1307
ユーザF	ユーザE (ユーザE@ZZ.co.jp)	2003.0330	未	1308

【図14】

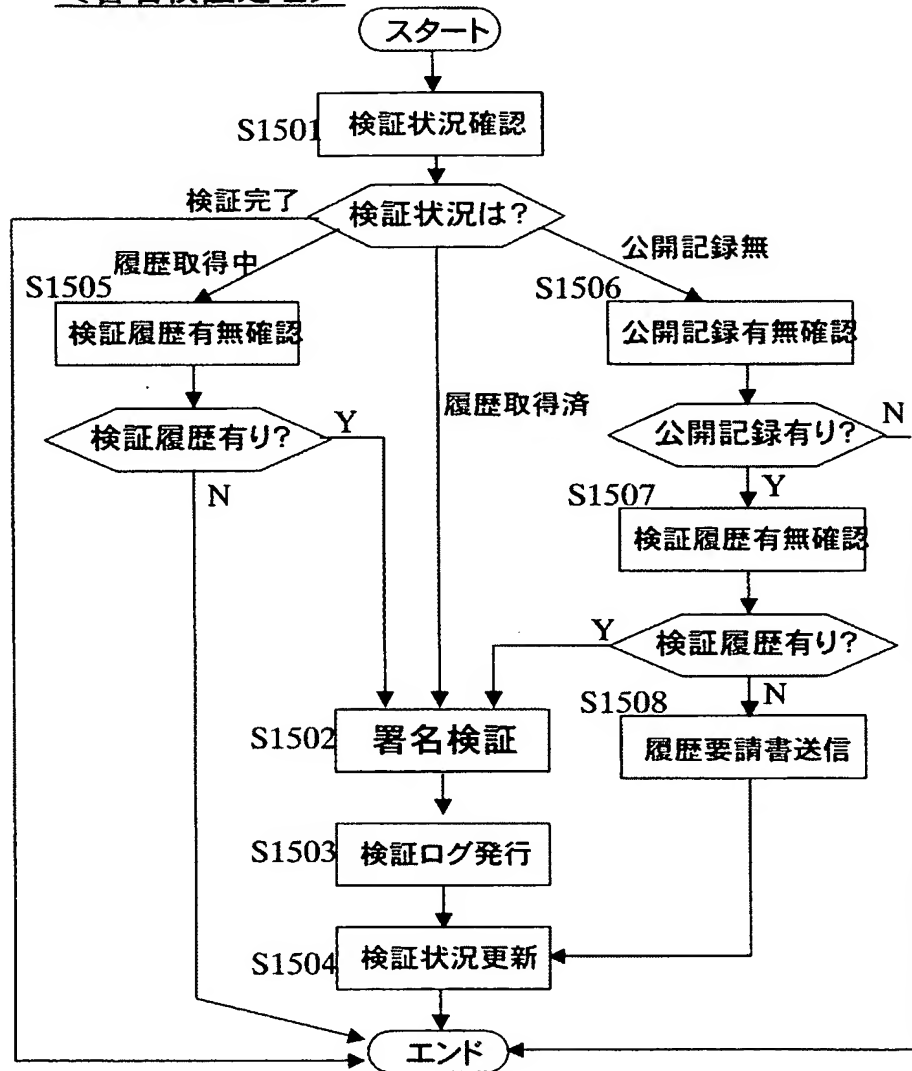
【図14】

検証代行サービス<検証代行依頼書受信処理>

【図15】

検証代行サービス 【図15】

<署名検証処理>



【図 1 6】

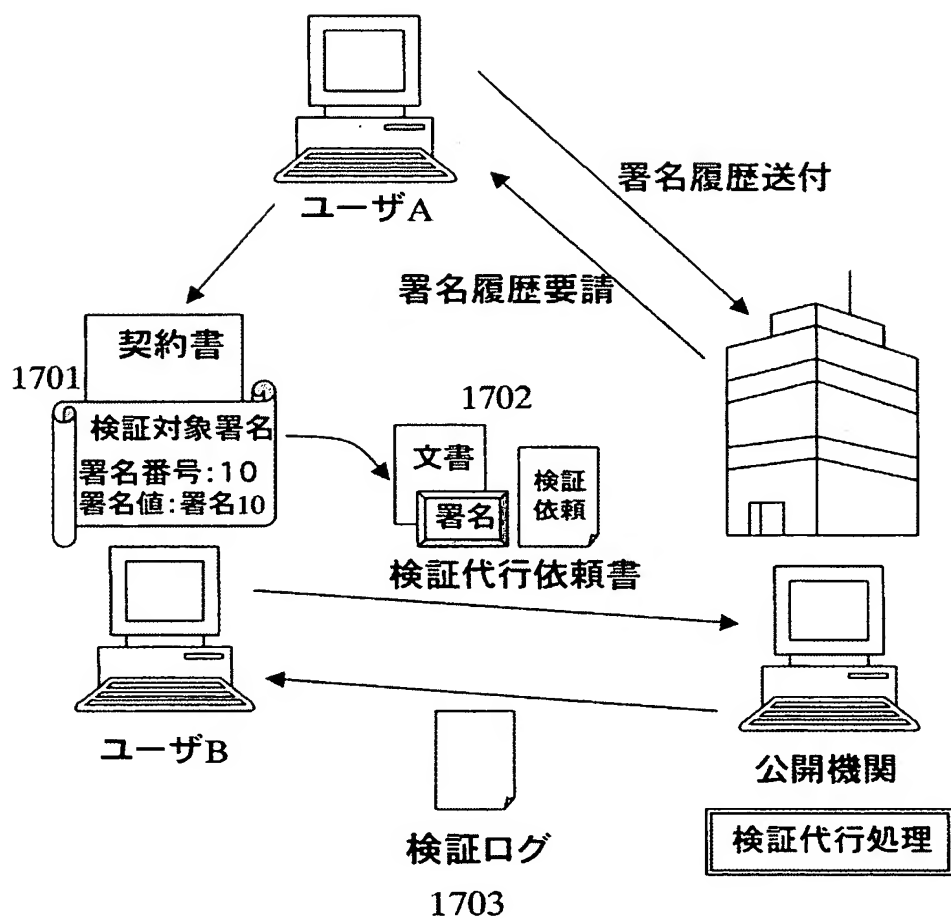
【図16】

1601 検証状況データベース

1602	1603	1604	1605	1606	1607	
検証ID	依頼ユーザ名 (メールアドレス)	検証対象署名者 (メールアドレス)	公開ID	依頼日	検証状況	
000001	ユーザB (ユーザB@XX.co.jp)	ユーザA (ユーザA@XX.co.jp)	000142	2003.0910	履歴取得中	1608
000002	ユーザC (ユーザC@YY.co.jp)	ユーザE (ユーザE@YY.co.jp)	—	2003.0511	公開記録無	1609
000003	ユーザD (ユーザD@ZZ.co.jp)	ユーザF (ユーザF@ZZ.co.jp)	000065	2003.0830	履歴取得済	1610
000004	ユーザG (ユーザG@ZZ.co.jp)	ユーザH (ユーザH@KK.co.jp)	000102	2003.0420	検証完了	1611

【図17】

【図17】



【書類名】 要約書**【要約】****【課題】**

ユーザ側装置に対して、検証した署名の証拠性を長期に渡って維持するための検証記録保存機能を提供する。また、公開機関側装置において、ユーザの署名の信頼性を保証するためのサービスを提供する。

【解決手段】

検証記録保存プログラムは、検証に使用した検証対象署名、署名履歴、預託公開署名記録を記録した検証ログを作成する。

また、公開機関側装置は、公開忘れの防止のための公開催促や、他のユーザの公開を知らせる公開通知や、ユーザに代わって検証の代行を行う検証代行など、信頼のある連鎖検証を確実にし、かつユーザの利便性も考慮したサービスを提供する。

【選択図】 図 7

認定・付加情報

特許出願の番号	特願 2004-028794
受付番号	50400185758
書類名	特許願
担当官	伊藤 雅美 2132
作成日	平成16年 2月 6日

<認定情報・付加情報>

【提出日】	平成16年 2月 5日
-------	-------------

特願 2 0 0 4 - 0 2 8 7 9 4

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 1 0 8]

1. 変更年月日 1 9 9 0 年 8 月 3 1 日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台 4 丁目 6 番地

氏 名 株式会社日立製作所